Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON THE DEPARTMENT OF DEFENSE'S ROLE IN PROTECTING DEMOCRATIC ELECTIONS

Tuesday, February 13, 2018

Washington, D.C.

ALDERSON COURT REPORTING

1155 CONNECTICUT AVENUE, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 289-2260

www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON

THE DEPARTMENT OF DEFENSE'S ROLE

IN PROTECTING DEMOCRATIC ELECTIONS

Tuesday, February 13, 2018

U.S. Senate

Subcommittee on Cybersecurity

Committee on Armed Services

Washington, D.C.

The subcommittee met, pursuant to notice, at 2:34 p.m. in Room SR-222, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Committee Members Present: Senators Rounds [presiding], Fischer, Sasse, Nelson, McCaskill, Gillibrand, and Blumenthal.

OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

Senator Rounds: Good afternoon.

The Cybersecurity Subcommittee meets this afternoon to receive testimony on the Department of Defense's role in protecting the U.S. election process.

The witnesses are Mr. Bob Butler, Cofounder and Managing Director of Cyber Strategies, LLC; Adjunct Senior Fellow at the Center for a New American Security; Senior Vice President of Critical Infrastructure Protection Operations for AECOM; Ms. Heather Conley, the Senior Vice President for Europe, Eurasia, and the Arctic and Director of the Europe Program at the Center for Strategic and International Studies; Dr. Richard Harknett, head of political science at the University of Cincinnati and a former scholar in residence at U.S. Cyber Command and the National Security Agency; and Dr. Michael Sulmeyer, the Director of the Cyber Security Project at the Harvard Kennedy School.

At the conclusion of Ranking Member Nelson's comments, we will ask our witnesses to make their opening remarks. After that, we will have a round of questions and answers.

There is no dispute about what Russia did during the 2016 election cycle. There is clear evidence that Russia attempted to undermine our democratic process through the

hacking of independent political entities, manipulation of social media, and use of propaganda venues such as Russia Today. Evidence to date indicates that no polls or State election systems were manipulated to change the outcome of the vote. However, there was evidence of Russian probing of certain election systems in 21 States.

The Department of Defense has a critical role to play in challenging and influencing the mindset of our cyber adversaries and defending the homeland from attacks, attacks that could include cyber attacks by other nations against our election infrastructure. We look forward to the Department approaching these issues with a heightened sense of urgency.

The threat is not going away. Just a couple of weeks ago, the Director of the Central Intelligence Agency warned that Russia will seek to influence the upcoming midterm elections. The White House National Security Advisor stated that the Mexican presidential campaign as well. This is all in addition to Russian attempts to influence the elections in France and Germany last year.

Each of us on this panel has been quite vocal about the need for a strategy that seizes the strategic high ground in cyberspace. Whether you call it deterrence or something else, we need a strategy that moves out of the trenches and imposes costs on our adversaries. The lack of consequences

for the countless attacks over the past decade has emboldened our adversaries and left us vulnerable to emboldened behavior. The attacks we experienced during the 2016 election are just the latest rung on that escalation ladder. As long as our adversaries feel that they can act with impunity, they will press further.

Our witnesses offer unique perspectives on the challenges we face. We look to them to help us understand why our posture restraint has not worked, if we can reverse the damage already done, and what it will take to develop and implement a strategy that limits our exposure and imposes costs on malicious behavior.

We invited Dr. Richard Harknett to explain his theory of cyber persistence, specifically on how our failure to tailor our strategies to the uniqueness of the cyber domain limits our ability to confront challenges we face. Our adversaries actively exploit us because they see great benefit and little consequence in doing so. I agree with Dr. Harknett that the Cold War models of deterrence will not work and look forward to hearing what he believes it will take to influence the mindset of our adversaries.

In addition to his writings on cyber deterrence and election attacks, Dr. Michael Sulmeyer has focused a great deal of his research on the organizational challenges we face as a government. We understand that Dr. Sulmeyer is

working on a paper addressing some of the challenges we examined during our full committee hearings in October on the whole-of-government approach to cybersecurity. We look forward to hearing more from Dr. Sulmeyer on the gaps and the seams he sees in our organizational model and what lessons we can learn from analyzing like the British.

Ms. Heather Conley provides an expertise in Russian politics and foreign policy. Russia has yet to face serious consequences in the cyber or other domains for its 2016 elections' interference. We look forward to Ms. Conley's testimony on how the United States can tailor and implement these penalties and how the Department can best deter or dissuade further Russian election meddling.

We also look forward to the testimony of Mr. Bob Butler who brings extensive cyber experience in both the Department of Defense and the private sector. Mr. Butler has been involved in numerous studies on the cyber deterrence, including the recent Defense Science Board Task Force on Cyber Deterrence.

Let me close by thanking our witnesses for their willingness to appear today before our subcommittee.

Senator Nelson?

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator Nelson: Thank you, Mr. Chairman.

First of all, I want to make sure that since this is a hearing on elections, that everybody understands that this Senator feels that this is about the foundation of our democracy and that we as a government ought to be doing more to defend ourselves.

And the second thing I want to make sure everybody understands is this is not a partisan issue. This can happen to either party or the non-party candidates as well. And it ought to be all hands on deck.

The chairman and I in public and in closed meetings because of the clearance -- we have been quite disturbed about wondering if we are doing as much as we should as a government to protect ourselves. So in a recent closed hearing of this subcommittee, the Department of Defense demonstrated that it is not taking appropriate steps to defend against and deter this threat to our democracy.

So, Mr. Chairman, I join you in welcoming these witnesses and hope that some practical suggestions are going to come out. Now, I want to mention just a few things.

First, the Department has cyber forces designed and trained to thwart attacks on our country through cyberspace, and that is why we created the Cyber Command's National

Mission Teams. A member of this subcommittee, Senator Blumenthal, Senator Shaheen -- we all wrote to the Secretary of Defense last week that they, the Department, ought to be assigned to identify Russian operators responsible for the hacking, stealing information, planting misinformation, and spreading it through all the botnets and fake accounts on social media. They ought to do that. The Cyber Command knows who that is.

And then we ought to use our cyber forces to disrupt this activity. We are not.

We should also be informing the social media companies of Russia's fake accounts and other activities that violate those companies' terms of service so that they can be shut down.

Second I would ask us to look at that as the Department's own Defense Science Board Task Force on Cyber Deterrence concluded last year -- we ought to show Mr. Putin that two can play in this game. We ought to consider information operations of our own to deter Mr. Putin like exposing his wealth and that of his oligarchs.

Third, I would suggest the Department should ensure that its active and reserve component cyber units are prepared to assist the Department of Homeland Security and the governors to defend our election infrastructure, not just after the attack but proactively before and during the

Russian attacks.

Fourth, I would suggest that the Department must integrate capabilities and planning to cyber warfare and information warfare to conduct information warfare through cyberspace as last year's defense bill mandated. Our adversaries recognize the importance of this kind of integration, but today cyber warfare and information warfare are separated in the Department of Defense and involve multiple organizations.

And fifth, I would recommend, as one of our witnesses I think will testify today, the Department must help develop an effective whole-of-government response to Russia's strategic influence operation through things like a joint interagency task force and a fusion center. Our colleagues on the Foreign Relations Committee have proposed something similar. The threat is not going away. It is likely to intensify. And as our intelligence community has been warning and as DNI Coats has just testified to the Senate Intelligence Committee, that threat is not going away.

So the 2018 elections are upon us. We cannot sit idly by and watch this happen again.

Thank you, Mr. Chairman.

Senator Rounds: Thank you.

And welcome to all of our panelists here today, our witnesses. We would ask that, first of all, you limit your

opening remarks to 5 minutes, but your entire statements will be made a part of the record. We would like to begin with Mr. Butler.

STATEMENT OF ROBERT J. BUTLER, COFOUNDER AND MANAGING DIRECTOR, CYBER STRATEGIES, LLC;

Mr. Butler: Thank you, Mr. Chairman, Ranking Member Nelson, and distinguished members of the Cyber Subcommittee. It is a privilege to be here. Thank you for the invitation.

My views really represent my views and not that of any particular organization. And I will just quickly hit the highlights of my written statement. They track very closely with a lot of the opening comments. My comments are really focused around my assessment of the threat in the electoral processes after interviewing a few different States; secondly, recommendations for the Federal Government partnered with a whole-of-America campaign; and then thirdly, what this subcommittee can do going forward.

I have been watching the Russian influence operations threat for some time in uniform and out of uniform. And our ability to counter Russian influence operations is not only a function of what we know about the threat but our willingness and our ability address that threat through hardening resilience and other countermeasures.

As I have looked at the election infrastructure in a few different States, we have learned from 2016, and our known vulnerabilities have been remediated. Whether you look at the voting registration systems in the election infrastructure proper, we are making progress there.

However, the States do not know how to address the disinformation campaign. That is a struggle and the threat still remains very, very high.

From my perspective looking at this particular threat, what we are talking about today is one line of operation within what I think has to be addressed through a National Security Council-led task force, a whole-of-America campaign not too much dissimilar from the NCTC, but with a strong, empowered private sector element. Again, I go back to the idea of a whole-of-America process.

Two key components inside of this. One is the idea of having an element that is focused on strengthening States' election infrastructure and hardening American citizens, deterrence by denial some would say. A second component focused on cost imposition from botnet disruptions to other kinds of sanctioning activities, importantly reinforce multilaterally. I am a big proponent of an international cyber stability board, a coalition of the willing, working to ensure the most effective way of doing cost imposition. Those two components then supported by an integrated fusion center that provides situational awareness, combines the best of intelligence both in the commercial and from the national security community with law enforcement and active defense actions, focused on a campaign that is centralized in its planning but decentralized in its execution.

From my perspective, it really requires both cultural and legislative enablers. Culturally the President must lead, must rally the nation. There are opportunities already this week that can be used to help with that. The infrastructure proposal is a great example. I do not see anything about resilience in the infrastructure proposal. We should have a way of incorporating, especially as we are building new infrastructure, methods and strategies and incentives for strengthening the infrastructure here in this country.

Additionally, we need to leverage the best of U.S. competencies across America. Defense is excellent at campaign planning and exercise. U.S. intelligence agencies, combined with web-scale companies, do a great job in intelligence generation and fusion. Web-scale companies are very good and growing in their ability to rapidly identify disinformation campaigns and response, and we will need some help from the legislative side.

Specifically for DOD, five recommendations that track very closely with what Senator Nelson was talking about. I think to jump start this NSC-sponsored task force, we should coordinate with the Secretary of Defense to immediately stand up a JIATF, a joint interagency task force. Inside of that, again empowered private sector players. We typically do not think about that, but this really is something where

we need to work together in a public-private partnership. We need to make arrangements with State and local officials through DHS and the National Guard Bureau.

The second recommendation really is to the NGB and working with the National Guard Bureau to really not only inventory what we have from a cyber and IO perspective. We have cyber units. We information operations units. But to begin to scale them to help the States and to help us as we think about incident response in general. I think they could be aligned with FEMA regions. I think they could be aligned in a lot of different ways, but we need to first get organized.

The third is to actually have a session where we discuss courses of action. It would have to be a closed session. But I think that is where the request for authorities, new authorities, requests for new resources come out. It really gets at the point of not only looking at offensive actions but defensively what we are in store for as we begin to move offensively and what we are going to do from a continuity of government, continuity of business perspective.

The last two relate to Senator Nelson’s comments with regard to the DSB task force. I think we should continue to push with the NDAA and operationalizing the rest of the Cyber Deterrence Task Force recommendations. And I would

advocate that this committee should have its own campaign of exercises to help it understand where the adversary is going and to be able to advance ideas with regard to looking at threat and countermeasures.

I stand ready to answer any questions that you have.

[The prepared statement of Mr. Butler follows:]

Senator Rounds: Thank you, Mr. Butler.

Ms. Conley?

STATEMENT OF HEATHER A. CONLEY, DIRECTOR, EUROPE PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Ms. Conley: Thank you so much, Chairman Rounds, Ranking Member Senator Nelson, and esteemed colleagues. Thank you for this very timely opportunity to speak to you this afternoon and what a timely moment as U.S. intelligence agencies have now assessed that Russia will continue to make bold and more disruptive cyber operations focused on the midterm elections. CIA Director Mike Pompeo also stated publicly that he fully expects that Russia will attempt to disrupt the U.S. midterm elections. So we know they are doing it and will do it, but we as a nation are not prepared to effectively combat what I believe is an intensifying disinformation operation and influence operation.

I am a bit of a contrarian on this panel. I am not a cybersecurity expert. But what I am most concerned about is that we have 9 months, and the American people are not educated as to what is going to happen to them. And that is where I think our focus must lie. I am less concerned about the mindset of President Putin. I know his mindset. I am more concerned about the mindset of the American people as we head towards this election.

You asked us what role DOD could play to protect the U.S. elections. And I think simply DOD, working with Congress, has got to demand a whole-of-government strategy

to fight against this enduring disinformation and influence operation. We do not have a national strategy. Unfortunately, modernizing our nuclear forces will not stop a Russian influence operation. That is where we are missing a grave threat that exists in the American people's palm of their hand and on their computer screens. It is vital that we start talking publicly about this threat and educating the American people on a bipartisan basis.

Tragically the Russian campaign has already deeply polarized our country, which only serves the Kremlin's interests. As one of the most trusted institutions in the United States, the Department of Defense must leverage that trust with the American people to mitigate Russian influence. Simply put, the Department of Defense has to model the bipartisan and fact-based action, behavior, and awareness that will help reduce societal division. This is about leadership. It is about protecting the United States, and as far as I can see, that is in the Department of Defense's job description.

So a good place to begin is using DOD's extensive employee and military networks to provide timely policy guidance and statements about the threat the Russian influence operation poses to election security. Secretary Mattis and General Dunford should provide extensive public outreach to the defense community about the threat and how

to counter it. Perhaps they should think about forming public service announcements. European governments have been very effective in warning their publics about the danger of Russian disinformation. France and Germany were very strong on that, but you have to put the message out and we have not.

I offered one suggestion in my written testimony to look at how we could leverage the National Guard Bureau, working closely with State and local leaders in cooperation with the Department of Homeland Security, to enhance cybersecurity awareness and be able to detect patterns of influence, for example, if packed emails surface online in conjunction with the false rumors about potential electoral candidates. We need to start talking about this.

Another instrument is the State partnership program. The National Guard has partnered with the Lithuanian military, the Estonian military. They can bring back to their States information about how Russian influence works.

We are speaking today about protecting the homeland from continuous disinformation attacks, which alter how the average American thinks about their system of governance and their government. And what the American people may end up thinking is that everyone is lying, everything is fake, and there is nothing that can be trusted. And then even the most trusted of American institutions, the Defense

Department, the Justice Department, the FBI, the Department of Homeland Security, the Office of the President, will mean very little to the American people. And this is exactly how you break the internal coherence of the enemy's system according to Russian military doctrine. And unfortunately today we are doing most of this to ourselves without assistance from the Kremlin.

This is a matter of urgency. We have 9 months. We need to educate the American people in addition to enhancing, of course, our cybersecurity protections. But as the French disinformation attacks showed, what many of the organizations that looked like that disinformation was coming from -- it was coming from American organizations. This is designed to be hidden. It adapts. We have to educate the American people about what they are going to confront on the November elections.

Thank you.

[The prepared statement of Ms. Conley follows:]

Senator Rounds: Thank you, Ms. Conley.

Dr. Harknett?

STATEMENT OF DR. RICHARD J. HARKNETT, PROFESSOR OF POLITICAL SCIENCE AND HEAD OF POLITICAL SCIENCE DEPARTMENT, UNIVERSITY OF CINCINNATI

Dr. Harknett: Chairman Rounds, Ranking Member Nelson, distinguished members, thank you for this opportunity to speak to you about this critical issue today.

We have a big picture problem. Throughout international political history, states have at times misaligned their security approaches to the strategic realities in which they tried to secure themselves.

In 1914, every general staff in Europe thought that security rested on the offense, and they found out devastatingly in World War I that they were tragically wrong.

France in the 1930's said, okay, we learned from the last war. It is a defense-dominant environment. We are going to rest our security on the most technologically advanced defensive works in history. But again, the fundamentals had changed and the Germans simply went around the Maginot Line.

Senators, with all due respect, I do not want to be France in the 1930s, but I think we are coming dangerously close to that myopia and the misalignment of strategy that follows from it. Our adversaries are working through a new seam in international politics. Cyberspace is that seam.

Its unique characteristics have created a strategic environment in which our national sources of power can be exposed without having to violate traditional territorial integrity through war.

What we have been witnessing are not hacks. They are not thefts. It is not even simple espionage. What we must accept is the fact that we are facing comprehensive strategic campaigns that undermine our national sources of power, be they economic, social, political, or military. And so, therefore, I agree we must develop a counter strategic campaign to protect those sources that has as its overall objective a more secure, stable, interoperable, and global cyberspace.

With regard to the integrity of our elections, we have effectively left civilians, whose main focus is not security, on the front lines. That is not a recipe for success.

Specific to the Department of Defense’s role in producing greater security in, through, and from cyberspace, we must adopt a seamless strategy of what I call cyber persistence, in which our objective is to seize and maintain the initiative. We must defend forward as close to adversary capacity and planning as possible so that we can watch and inform ourselves, disrupt and disable if necessary.

Our immediate objective must be to, first, erode the confidence adversaries now have in their ability to achieve and enable objectives. They are very confident.

Second, we have to erode their confidence in their own capabilities.

And third, we must erode those capabilities themselves.

We are well past the post on this. We need a comprehensive, seamless, integrated strategy that pulls to get a greater resiliency, forward defense, and when necessary, countering and testing cyber activity to reverse current behavior. We are not at step one. We are well past that. We actually have to reverse behavior.

Our security will rest on our ability to simultaneously anticipate how adversaries will exploit our vulnerabilities and how we can exploit theirs.

Cyberspace is an interconnected domain of constant contact that creates a strategic imperative for us to persist. This is a wrestling match in which we have to grapple with who actually has the initiative, being one step ahead in both knowledge and in action. If we do not adjust to this reality, our national sources of power will remain exposed and more of those who wish to contest our power will pour into this seam.

I, therefore, argue that we must make three critical adjustments.

The first is we have to adjust our overall strategic perspective. War and territorial aggression, which can effectively be deterred, are not the only pathways for undermining our national sources of power. In fact, because we have this effective strategic deterrent, we should expect our adversaries to move into this new seam of strategic behavior below the threshold of war.

Second, we must move our cyber capabilities out of their garrisons and adopt a security strategy that matches the operational environment of cyberspace. We must meet the challenge of an interconnected domain with a distinct strategy that continuously seeks tactical, operational, and strategic initiative.

Third, we must make the fundamental alterations to capabilities development, operational tempo, decision-making processes, and most importantly, as Bob referred to, overall authorities that will enable our forces to be successful. We cannot succeed using authorities that assume territoriality and segmentation in an environment of interconnectedness, constant contact, and initiative persistence. We cannot secure an environment of constant action through inaction. Strategic effect in cyberspace comes from the use of capabilities and having the initiative over one’s adversaries. It is time for us to seize that initiative.

I look forward to explaining in more detail how we can pursue security through persistence during our Q and A. Thank you, Mr. Chairman.

[The prepared statement of Dr. Harknett follows:]

Senator Rounds: Thank you, Dr. Harknett.

Dr. Sulmeyer?

STATEMENT OF DR. MICHAEL L. SULMEYER, DIRECTOR, CYBER SECURITY PROJECT, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD UNIVERSITY

Dr. Sulmeyer: Thank you, Chairman Rounds, Ranking Member Nelson, and distinguished members of the subcommittee. It is an honor to be with you today.

Before I get to the military's role, however, I would like to note that I am part of a team at the Kennedy School's Belfer Center that released a report a couple hours ago. It is a playbook for State and local election administrators, and it has got steps they can take to improve the cybersecurity of systems that they administer. It is based on field research by a wonderful research team. Many, many students contributed. I am very lucky to have one of the wonderful students here with us today. Corina Faist has flown down to join us.

So regardless of the role of the Department of Defense, these defensive improvements are essential. And I want to make sure I hit that right up front. Those recommendations that we put out today complement our last playbook for political campaigns to also improve their cybersecurity. It is essential that we make our elections harder to hack and that we improve resiliency in case critical systems are compromised. But we should also consider how best to counter threats abroad before they hit us at home.

So let me transition to how I see some potential roles for the military outside of the United States to protect our elections. There are two necessary conditions of posture that I see as critical: reconnaissance posture and force posture.

First, reconnaissance posture. Our cyber mission forces should constantly conduct reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to address all threats equally, so prioritizing threats to our democratic processes is critical. Otherwise, we cannot hope to disrupt these threats.

On force posture, our forces must be sufficiently ready to strike, strike against targets abroad that threaten our elections. Readiness is a critical issue for our armed forces today, and I would encourage Senators on this subcommittee to ensure they are asking tough questions about the readiness of our cyber forces just as they would about any other part of our military.

And if the military's reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that I think our forces should be prepared to pursue. It should go without saying that undertaking these actions should be consistent with

international law and other relevant U.S. commitments.

Those objectives are: first, preventing attacks from materializing; second, preempting imminent attacks; third, halting attacks in progress; and fourth, retaliating, if necessary, after an attack.

On the fourth, let me just note I would emphasize that this retaliation needs to be timely. It has got to be timely since the more time that elapses after an adversary's initial attack, the harder it will be to message and communicate that our action is a direct response.

Across those objectives, proper training, thorough rehearsals, and coordination with other parts of our government are essential. Bringing military capabilities to bear inside or outside of cyberspace is always a serious matter, so it is critical to ensure that rules of engagement and questions about authorities are settled well in advance of any order to strike. Here, I would note that some of our closest allies like the United Kingdom and Israel have undertaken some national-level organizational reforms to streamline responsibilities for cyber issues. And we may at some point want to consider something similar here.

One of the best cyber-related investments the nation has made is in the national mission force, an elite group of network operators at Cyber Command. They defend the nation from an attack of significant consequence in cyberspace. I

think it is very much worth considering what role the NMF can play to accomplish the objectives I described just now.

I might note for Senators that I have not discussed deterrence much so far. I very much support calls to deter our adversaries from meddling in elections. Do not get me wrong. However, I would not want to bet the cybersecurity of U.S. elections on a policy of deterrence if I did not have to. Sometimes, like the prospect of defending against thousands of nuclear-tipped missiles, deterrence is the least bad option. That is not the case in cybersecurity. We have other options, like the ones I described just now, and we should employ them alongside strong policies of deterrence.

Finally, I would just note that information derived abroad from reconnaissance should be shared with relevant parties at the State and local level. I want to commend the Department of Homeland Security for working hard to promote information sharing over the last few years.

And I would also like to encourage more thinking, especially among my colleagues in academia, to help Congress protect itself since Congress is so critical as a part of our democratic process, not just work accounts but also campaign accounts, personal accounts. These cannot be left vulnerable.

That concludes my prepared testimony. I look forward

to taking your questions.

[The prepared statement of Dr. Sulmeyer follows:]

Senator Rounds: Thank you, Dr. Sulmeyer.

First of all, let me thank all of you for some great insight, and I look forward to your thoughts in terms of the questions that we ask.

What I would like to do is to do what we call 5-minute rounds here. We will alternate back and forth. And then after we have done that once through, if we have time, I would go back through and do a second round depending upon the amount of time that we have and whether or not other members come.

Let me begin with mine. I am going to start with Dr. Harknett. You have written that restraint and reactive postures are not sustainable, that the United States needs a strategy that capitalizes on the unique attributes of the cyber domain. You have called for a strategy of cyber persistence where we are constantly engaged with our adversaries seeking to frustrate, confuse, and challenge.

How would your strategy calling for persistent engagement apply in the Russian meddling with our election as an example? And should this involve us contesting the malicious behavior at its source? And what do you believe are the consequences of our failure to respond in cyberspace to the Russian election interference? Because, number one, we have got to be able to provide attribution to where it is coming from, and hopefully we have got that completed. But

give me your thoughts on it. What would you say would be an example of persistent engagement with regard to what they have done already and what we expect them to do?

Dr. Harknett: Thank you, Senator.

So let us think about the Internet Research Agency. Right? I mean, we know about this center in St. Petersburg. We know that it controls a series of automated bots that are driving particularly well conceived information operations that are meant to be divisive. I do not know why we are according or why we should accord First Amendment rights to bots. It is not a free speech issue. If we have evidence of foreign manipulation, technical manipulation, of the social media space, that is not what the American people, from an educated standpoint, actually understand is coming at them. They think that this is a majoritarian aggregator trending. It is telling me, hey, this is where everybody is going. But if that trend is being driven by automated foreign intrusion, that is not an issue over free speech. That is an issue of direct foreign manipulation.

And so I agree with Dr. Sulmeyer. We need to have the reconnaissance, to your point about attribution. That is what persistence enables you to do, to start to get better at attribution. But we need to be able to move at the speed of relevance. So if in fact those bots are hitting us in a particular trend that is meant to be divisive, we should be

able to have the capacity to at least disrupt if not disable that capacity.

So we do know where some of these capacities lie. By being persistent in our reconnaissance, we will get a better understanding of what our vulnerability surface is. We have to think about it that way. We tend to think about an attack surface. That is from their perspective. We have to get a better handle on what our vulnerability surface is. And by being able to understand where our vulnerabilities are and anticipate where their capabilities map to that, again, a product of being persistent in this space, we can start to take those capabilities away.

Senator Rounds: Dr. Sulmeyer, do you agree with that?

Dr. Sulmeyer: I do. I agree with the vast majority of what my colleague, Dr. Harknett, just said.

For me, even just to get a little more specific, the kinds of options that I would want to be seeing presented need to allow decision-makers some flexibility from lower-level actions like denying troll farm access to compromised infrastructure, to deleting some accounts, to erasing some systems if it comes to it. It is too important to take options off the table ahead of time. So as long as the option space is kept open, we can do it persistently or less persistently, but a wide range of options.

Senator Rounds: Mr. Butler, your thoughts.

Mr. Butler: I agree with both Michael and Richard on this. I would say that we need to be asymmetrical in our response. So I am a big believer in botnet disruptions and taking down bot infrastructure, as we just saw with Levashov, but we need to do that in a continuous way and that is a symmetrical response.

I think if you look at the Internet Research Agency in St. Petersburg, they are coupled to the Kremlin. You need to have an information operations counter-influence campaign where you begin to cut the funding and cut the support enablers behind that infrastructure. So we need to think about things differently. It should not be cyber on cyber, social media on social media. It has got to be a broader campaign.

Senator Rounds: Ms. Conley?

Ms. Conley: Yes. I will agree with absolutely the asymmetrical response. And while trying to bring down the infrastructure of those bots, what they are doing, though, Russia exploits the weaknesses that it finds. So it is amplifying the weaknesses and divisions that are already appearing on social media. So how do we try to reduce the weaknesses?

And this, again, gets back to the critical importance of exactly what this committee represents, the bipartisanship, fact-based, and getting to communities

through a variety of methods to help inform the American people so when they see a trending site, let us look at that. What is underneath that? The only way we can really stop this from changing hearts and minds among the American people is helping them discern what is coming. We can do everything we can technologically to eliminate it. But the other part is just missing. We are not educating.

On the asymmetrical sanctions, my frustration -- and I am sure many on this committee as well --

Senator Rounds: I am going to ask you to shorten it up because my time has expired.

Ms. Conley: Absolutely, sorry about that. Is to think about ways that we can focus on the Kremlin, on financial sanctions, on sanctioning the inner circle as ones attributable back to that, so not just in the cyber domain, focusing on financial sanctions and individual sanctions. That could be very powerful as well.

Senator Rounds: Thank you.

Senator Nelson?

Senator Nelson: So all of you sound like that you just do not think enough has been done and that we are not ready. And, Dr. Harknett, you have said that 2016 was the Stone Age compared to what is going to happen. So do you want to trace what you think will happen?

Dr. Harknett: Well, one of the things, back to the

chairman's question about whether the lingering effects, is again we have got adversaries who are confident. There are other actors aside from Russia out there as well that are going to look at this space and say, hey, this is a space that I can play in and I can work in. And so until we start to reverse that confidence, we are going to see greater experimentation.

Technologically, I will give you one example, Senator. My concern with regard to leveraging artificial intelligence and machine learning. I mean, this will be a step function, thus my Stone Age allusion, from where we are. We are going to -- within the next 16 months, I am going to be able to take you and put you in a video in which you are saying something that you never said in a place that you have never been, and you are not going to be able to authenticate that you were not doing -- that you had not done that and not been there. Just think about that as a tool for an adversary who wants to engage in disruptive social cohesion types of information campaigns.

Senator Nelson: Right.

Dr. Harknett: That is around the corner.

Senator Nelson: So, Ms. Conley, given that, you have already said that you do not think we have taken any positive proactive steps. Why do you think that is the case?

Ms. Conley: I think the executive branch refuses to recognize the threat. It refuses to put forward a national whole-of-government, whole-of-society strategy and bring all the agencies and tools of influence to bear on this. We have to think of this as a direct threat to the national security of this country. It has to receive the priority.

Also, to focus on what Dr. Harknett said, this is adaptation. If we are preparing for what Russia did in 2016, it will be very different in November. It will be very different in 2020. It will look more American. It will look less Russian. And so this is adaptation. We are already fighting the last war. We are not ahead of the new one, which is why I think education is so critical, that absent a U.S. Government approach, we are all going to have to do our part in our communities to inform the American people about the threat. It is unfortunate we cannot pull together and do this in a unified way.

Senator Nelson: So if we cannot get the government to move, are there any private initiatives that would help?

Ms. Conley: What I am seeing is some very effective news literacy campaigns. I think, again, news sources, social media are doing fact checking. The pressure that Congress has brought to bear on the social media companies is changing their perspective. But, again, we are so late to need. This has been ongoing. This campaign is only

intensifying, and we are just getting our arms wrapped around this. So this is where every Member of Congress has to return to their home district and talk about this in very clear ways.

Senator Nelson: Amen to that.

And, Dr. Harknett, on the example that you gave of the next level of technology, of which something can be created that looks real, acts real, feels real, et cetera, if Cyber Command were to adopt your thinking, knowing what the threat is even greater in the future, what would you suggest that they change the way that they are doing their operations?

Dr. Harknett: I think it is very important to expand this notion of defending forward, this notion that we need to be as close to the source of adversarial capability and decision-making as possible. This is not a space in which time and geography is leveragable for defense. So when we think about the notion of front lines, the front lines are everywhere. And right now, our general approach has been to defend at our borders, at our network, which actually means that we start defending after the first breach, and we are already playing catch-up.

So I concur with the notion of adaptability here. It is all about anticipation. So when Bob Butler talks about asymmetric, that is what I would talk about in terms of being able to be one step ahead. We have to be able to

anticipate the exploitation of our vulnerabilities. You need to be able to be defending as far forward as possible. In terrestrial space, we defend forward. We are not defending forward in cyberspace right now.

Senator Nelson: Thank you.

Senator Rounds: Senator Gillibrand?

Senator Gillibrand: Thank you, Mr. Chairman and Mr. Ranking Member, for having this hearing.

Thanks to all of you for your testimony. I agreed with a lot of it.

So to Professor Harknett, I appreciate your effort to redefine cyberspace and the challenges we face in operating within it. Were Russia to have bombed one of our States rather than attacked our election infrastructure, we would treat it just like an attack, as you said. But because of the way in which we set up our cyber capabilities, which we have done for good reasons, including privacy and States rights, it seems to me that the DOD is hamstrung in trying to properly respond to an attack on our democracy.

I have asked this in many settings, and every single time they said it is not our job.

So you argue that we need to consider authorities that allow DOD, DHS, and our intelligence community to employ a coordinated strategy of cyber persistence and recommend looking at approaches emerging among all of our allies. Can

you expand on what kind of authorities we should be considering and what we might learn from our allies?

And I ask this because I have put this question to the Department of Defense in every setting we have had, any conversation about cyber, and every response is we do not have the authorities and the States rights issue. It is not our job. And I cannot, for the life of me, understand why they do not see it as their job because if another country bombed any one of our States, then that is a declaration of war and we would have responded from the military. We are not doing that in this regard, and it seems really off-putting to me. Their response is often, that is Homeland Security's job. They can call us if they need us, but they have not. I understand why that is probably not the case because of a lot of secretaries of state in a lot of States think it is their job, not anyone else's job, and they do not want to relinquish that control.

So I would like your suggestions on how to write the authorities that you think are necessary, but also I have really tried to push National Guard as a possible place where this can be done because the National Guard already serves the States. They are already under control of the governors. So why not amplify what we are already doing with our National Guard and Reserve to give them the expertise in cyber but actually delegate this mission

specifically to them in conjunction with all the other assets in the military?

So to all of you, you can answer this question. You start, Dr. Harknett, since you addressed it a little bit in your opening remarks about what authorities can we give. How can the National Guard be useful, and how do we get this done? Because it is frustrating to me that we are not doing it.

And then just a third thing to add to your answer. I do have a bill with Lindsey Graham to do a 9/11 deep dive style analysis of the cyber threat to our electoral infrastructure. It is a bipartisan bill. You know, whether we ever get a vote on it, I will never know, but that would be a great first step in my mind to at least just get a report and say these are the 10 things you need to do to harden our infrastructure. So maybe comment on those three ideas.

Dr. Harknett: Thank you, Senator.

You mentioned our allies, and I think Michael had some work that he has been doing as well analyzing them. I think if you look at the UK, for example, you look at the Israelis, you look at the Australians, their first default in cyberspace is to ask how do we find synergy, not segmentation. Our entire approach to this space has been starting with who has divided roles and responsibilities.

So I think we can learn something from our allies right now in terms of their orientation to trying to find synergy rather than segmentation. That should be our first policy framework question.

But in terms of authorities, I think there is a false debate, say, for example, between 10 and 50. So when I argue for a seamless notion, I am suggesting that we understand title 10 and title 50 as actually mutually reinforcing, not defined as, again, segmentating. They segment in Congress in terms of oversight, and I get that, but they do not segment in operational space. And so we should actually understand and reinterpret, I would argue, those authorities to emphasize where a synergy and where there is seamless reinforcement rather than looking at those authorities as something that divides and puts us into different lanes.

In terms of the National Guard, I think the cyber protection teams and force type of an approach would be appropriate. We need to get at this, Senator. So if that is the best mechanism, there is expertise at that level.

And Ms. Butler has talked about leveraging our private sector. Through National Guard, as well as Reserve, we have a capacity. If you look at the Brits, they are looking at cyber civilian reserve force. I think that is another interesting way of thinking about this.

So ultimately if we need to do a deep dive, I think we do. Right? I think we have authorities that are structured for a terrestrial space that does not map to the realities of this human-made interconnected space. Authorities are what we should do last. We should figure out what our mission is. We should develop the organizations to pursue those missions, and then we should authorize them to do it.

I would submit to you that one of the major problems that we have faced is we have been continually trying to shoehorn our cyber forces into existing authorities and working backwards from the way we should be working.

Senator Gillibrand: Ms. Conley?

Ms. Conley: Senator, I think the National Guard is an area that we absolutely should explore, and I mentioned it in my written as well as far as education, bringing together DHS, DOD, working with community leaders at the State and local level.

On the 9/11 Commission style, cyber is critical pillar of this, but it transcends it as well. We need to look at Russian economic influence. We have to look at a whole range not just of Russia as the adversary but other adversaries that will use cyber disinformation and economic. So please broaden that out. They will find any seam, State, federal, First Amendment, privacy. That is where they will be, and that is why we cannot get locked into those seams.

Mr. Butler: Senator, I take it from two different angles. One is clean-sheet everything. What do you want to do? And let us refocus the authorities. Catherine Lotrionte's work here in looking at countermeasures is a great example of that. Her legal interpretation of the Tallinn Manual is very different than what most people are saying these days.

The other thing is I am involved in exercises where I am blending physical and cyber together and looking at what we can do with physical authorities in cyberspace. So I am working with the Army Cyber Institute on an activity where we have a natural hazard and a nation state actor is manipulating inside of it. How do you get a rolling start? You can use our authorities. The military has the ability to use an immediate response authority to create a rolling start. We need to leverage. We need to reinterpret and leverage these kinds of things as we go forward.

A part of that is the National Guard Bureau. We have unevenness within the stand-up of our National Guard activities both in the air and now with the Army. We have both cyber and information operations. I think we could create pockets of talent. I mean, Washington State has a phenomenal industrial control system security unit. Maryland has a fantastic unit where they leverage a lot of NSA expertise. We have got units spread around the country.

We need to create a construct of cyber mutual assistance across boundaries, across State borders. And, again, I think we can do that. We have just got to sit down and plan together a campaign in that regard.

Senator Rounds: While the Senator's time has expired, if you could expedite your answer, we will let you finish up as well, sir.

Dr. Sulmeyer: I will go real quick. I support all the goodness just said.

Abroad, I do not believe the kinds of activities I described earlier need new authorities.

On the deep dive, I would say great. The Belfer Center's work over the last year has tried to get a start on that. So we hope we can be of support.

And on coms and education, there is a part of me that wonders if that by saying "cyber," the response is help desk. And by not describing it in a way about warfare and propaganda and foreign influence, we do a disservice to the real problem.

Thank you.

Senator Rounds: Senator Blumenthal?

Senator Blumenthal: Thank you, Mr. Chairman.

I want to thank all of you for being here. I am very familiar with the work done by the Belfer Center in particular, and thank you all for the work that is done by

each of your organizations.

I want to first tell you -- you probably already know-- that the immediacy and urgency of this task was reinforced this morning before the Senate Intelligence Committee where Dan Coats, the Director of National Intelligence, said, quote, there should be no doubt that Russia perceives its past efforts as successful and views the 2018 midterm elections as a potential target for Russian influence operations. That statement would be beyond conventional wisdom. It would be unnecessary to state because it is the consensus of our intelligence community. It has been broadly accepted by everyone except the President of the United States. And in my view that is the elephant in this room, that the President refuses to acknowledge this threat to our national security.

So I put that on the record simply because we can propose all the great ideas in the world. And some very good ideas, as a matter of fact, came from a report done by the Senate Foreign Relations Committee. It is a minority report by my colleague, then-Ranking Member Senator Cardin, called “Putin’s Asymmetric Assault on Democracy and Russia and Europe Implications for U.S. National Security.” It makes some very good proposals.

I would be interested to see the Belfer Center’s release today, and in fact, without even having seen it, Mr.

Chairman, I ask that it be made part of our record.

Senator Rounds: Without objection.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Blumenthal: But I think we need to make progress on gaining acceptance at the highest levels of the United States Government -- let me put it as diplomatically as possible -- for the proposition that Russia attacked our democracy. In my view it committed an act of war. They are going to do it again unless they are made to pay a price for it, and that includes enforcing sanctions passed overwhelmingly by this body 98 to 2, still unenforced. So the talk about retaliatory measures in real time, Dr. Sulmeyer, I think is very well taken. But why should the Russians take us seriously when the President denies the plain reality of their attacking our country and the sanctions that would make them pay a price are still unenforced?

All of that said, I want to raise another topic, which I think so far has been untouched, the social media sites, Facebook, Google. Let me ask each of you if you could comment on what their responsibilities are and how they are meeting them in this disinformation, propaganda campaign using bots and fake accounts which have been appearing on those sites. Mr. Butler?

Mr. Butler: I think, Senator, the response -- and I have talked with a couple of the web-scale companies about this -- is aligning with what we have already seen in the counterterrorism fight. And so in that space what you see

is them actively, proactively looking for disinformation, in the case of terrorism, of course, looking for recruitment. I think the challenge is guidance with regard to counter-narratives or alternative narratives in that space. That needs to be done with others. But I think that is where we need to head. They have the ability based on their reach and their fusion engines to really help us move much more quickly into active defense in this space and not just to do it from a cyber perspective but from a counter-influence perspective which I think is so critical.

Senator Blumenthal: Thank you.

Ms. Conley?

Ms. Conley: Thank you, Senator.

I would just note that building the awareness of what Congress has already done to force the social media companies to really take a very deep look at this has been very helpful.

I would suggest to you that I think Russia will adapt their tools, that this will look more and more American, which will get more and more into First Amendment issues because that is a weakness to exploit here.

So what I would commend, in the interest of being ahead of the curve and not behind it, is we start looking at how social media engines can start detecting what looks like it is American origin but it in fact is not. So that would be

the next step I would recommend.

Senator Blumenthal: Thank you.

Dr. Harknett: I think we have to move away from a partnership model, to be perfectly honest with you. We have been talking about a public-private partnership for 25 years. I published about this 25 years ago. And the problem is that partnerships require shared interest in the beginning of the morning. The private sector has a very specific interest: profit making. The state has a very specific interest: security providing. We should recognize and grant that they have a different interest.

And so we need to move us to an alignment model. How do we structure incentives within the marketplace for them to achieve their primary objective, which is profit making, while producing an effect that the state requires, which is enhanced security?

And until we actually start to actually think about how can we shape and incentivize that behavior and recognize that we actually have very different interests in this space-- I mean, that is Strava fitness band company a few weeks ago produced a heat map that exposes all of our forward-deployed troops. I would submit to you that nobody at their board meeting, when they came up with this really great idea of releasing that heat map -- and they said, look, our stuff is in the real dark places, and they thought

that was really cool. 10 years ago, the intelligence capacity that a state would have had to have found all of our forward-deployed troops -- think about that. And this was produced by a fitness company.

There are non-security seeking, security relevant actors in this space. That is the way we have got to think about them. Let us meet them on their grounds and start to get them to align towards the security needs that we have.

Senator Blumenthal: Thank you.

Dr. Sulmeyer: Briefly I would just note the interests are not aligned, and that is really the most essential part and to not treat them all the same. Not all the companies have gone through the same amount of self-reflection. Some have not; some have. And we should be honest about that.

And finally I do not think we should limit this to social media companies. There is a lot of companies up and down the stack, a lot of different types of people on the Internet who have an interest in this type of work.

Senator Blumenthal: Thank you all.

I apologize, Mr. Chairman. I have gone over my time.

Senator Rounds: What I would like to do is another round. Okay? Let us do it this way. Let us do one more round so that everyone has an opportunity. We will make it 5 minutes. And I would simply say that for those of us up on this end -- and I went over as well -- let us phrase it

so that when we hit the 5 minutes, whoever is final speaking on it will have their -- that will be the last one and we will move from there.

So with that, let me just begin with this very quickly. Right now, we are looking at changing our hats, our dual hats. Right now, within the cyber community, we have a dual-hatted individual for both title 10 and title 50 operations and so forth. We are looking at separating those into separate items: title 10 one side, title 50 on the other. The cybersecurity side would be separated out from the NSA side and so forth. We had a lot of discussions over it. We were concerned at first that they were going to go very, very rapidly. Now there is the discussion about whether or not moving in this particular way is quick enough.

I just want to know your thoughts about whether or not we are actually approaching the challenges that are facing us in the right way with regard to the organization of government as a whole. Can I just very quickly go across and just ask each of your thoughts about whether or not we are moving in the right direction as to how we are arranging so that we can respond to these types of threats? I will begin with Mr. Butler.

Mr. Butler: Thank you, Senator.

Let me start with the CYBERCOM/NSA issue. My sense is

we are at a point where we have got enough of the infrastructure developed to really work within Cyber Command, that we are not as dependent as we once were on the National Security Agency.

I think the other part of this is as we move forward with the kinds of influence strategies that we are talking about, we need to have a way of checking and understanding whether it is working. And so we need an activity that understands this space that can help Cyber Command make adjustments along the way.

So I support the split and support where we are trying to go as we move forward. And as we take a look at those two elements and we put it into a larger DOD IC and whole-of-government, whole-of-America construct, I go back to what I put in my written statement. I think from my perspective, having been through this both in uniform and doing information operations campaign planning and where we are today, we need to get the best of America into this space. There is a role for DHS. The FBI is very engaged. There is a role for the Department of Defense that goes beyond the National Guard Bureau that ties in with the intelligence community. There is a role for trusted private sector partners in this space. As a matter of fact, you cannot scale without it. So I think we have to align.

Senator Rounds: Thank you.

Ms. Conley?

Ms. Conley: The organizational structure gets to the reason why we needed a comprehensive 9/11-type commission because we are horribly structured for this particular challenge. It falls within the streams of law enforcement, intelligence, defense, education, awareness, and that is why we need a deeper dive to get to a reconfiguration. Just as we did after 9/11 with the DNI and DHS, we restructured ourselves. We need to do that again.

Senator Rounds: Thank you.

Dr. Harknett?

Dr. Harknett: I fully concur that we should do that deep dive, and I would urge us to reconsider the split of the dual hat. And I know that that is not the current view. This notion of my litmus test. Are you producing more synergy or are you producing more segmentation? There is not one of our allies that is moving in that direction.

Senator Rounds: Let me just ask one question on that very quickly because one of the items was is that we know that on the title 50 side, on the NSA side, they love to be deeply embedded and they do not want to be seen. There is a real concern out there that if they actually actively and more persistent that they are constantly being seen, that that interrupts their capabilities to be the intelligence gatherers that they are. How do we then allow for that

constant and persistent activity if they have the same concern about they would really rather not been seen? They just simply want to be the deep ears for us.

Dr. Harknett: So I think having the dual hat enables that kind of determination to be made. The sensitivity of both when and where we are going to make certain tradeoffs and where that seamless between intelligence and --

Senator Rounds: But it is not working today. Is it?

Dr. Harknett: No. I think it can. I think it can, sir.

Senator Rounds: But we do not have evidence.

Dr. Harknett: But if you look at our adversaries, why are they not worried about burning capabilities? Why are they not worried about -- we have had a high-end right kind of focus to all of this both in the recon phase and in the force phase that I think has actually been distorting of this space.

Senator Rounds: I am going to move over very quickly because Dr. Sulmeyer has been shorted each time around here.

Dr. Sulmeyer: You always pick on the Harvard guy.

[Laughter.]

Dr. Sulmeyer: I think we are back to different interests. The two different institutions have matured and now they have different missions, different jobs to do. And the current structure, what you can say for it, is very

efficient decision-making because it is one person who makes the decision. I think it is time, though, for two different and for an adjudication to be made for which priorities are going to take precedence each time.

Senator Rounds: Thank you.

Senator Nelson?

Senator Nelson: But until we evolve into that new structure, we are stuck with what we have. And we set up these Cyber Command national mission teams to disrupt the Russian troll farms, the botnets, the hackers, all engaged in attacks on our democracy, re the elections. And we can identify them, the infrastructure they use. We can identify their plans, their operations. We can do everything that we can to stop these activities, but if you do not do anything, it is not going to happen. And until the existing structure that we have -- the Secretary of Defense walks into the room and says, boss, and his boss is the commander-in-chief -- until he says, boss, we have got to act, nothing is going to get done.

So are we describing a situation that we are defenseless in this 2018 election?

Mr. Butler: My sense, sir, is no. My recommendation is, in the homeland defense mission of the Department of Defense, we should stand up a JIATF and move forward as we begin to move to another level, which would be a national

security task force. But in the interim, this committee has jurisdiction. The Secretary has prerogatives to set up a JIATF in support of homeland defense. This is a homeland defense issue.

Dr. Harknett: I would just add one. I think it is a defend the nation issue.

Senator Nelson: I think you are right. I think this is as clear an attack on the country as if you lobbed a missile or if you lobbed an artillery shell.

Senator Blumenthal wanted to ask the question. One of you had stated that it is going to morph into where the attacks are going to look more American. Would you expand on that, please?

Ms. Conley: Senator, that was me.

It is in part from some of the lessons we learned from the French presidential election. The last cyber attack, which happened within the last 24 hours of the campaign -- it was a combination of both hacked emails from Macron's campaign, as well as made-up messages, and it was all mixed in between. What we understand -- and I do not have access to classified briefings from our French colleagues -- where the source came from looked like it was coming from the United States, from U.S. organizations. And some of this is tied into adaptation where they do not want it to look like a Russian bot. They do not want it to look Russian. They

wanted to originate from other sources to confuse and make attribution questionable in those last few moments.

So my intuition tells me that more and more of these attacks will look like they are coming from America. It will obscure attribution, and then people will say this is their First Amendment right to say these things and put forward these -- that is the problem.

Senator Nelson: And how did the French counter that?

Ms. Conley: Well, very gratefully, the French have a very unique -- they have a blackout period 24 hours before an election. It is a reflection period. And because the French government and intelligence agencies had made very clear repeatedly and publicly that this was likely to happen, French media were very responsible. They could not fact check the material in time. The reflection period would not move forward. And in fact, that last major attack was really thwarted because both of a law but also a lot of French proactive steps to inform their public that this could happen.

Senator Nelson: And that was in the last 24 hours before the French election.

Ms. Conley: So what had happened, it was the presidential election debate between Marine Le Pen and Emmanuel Macron. It was the Wednesday before the election on Sunday. And in that debate, she began to hint that there

may be some information about potentially Mr. Macron's overseas bank accounts and sort of hinted at this. Then about 24 hours later, the document release happened. So one could speculate that there was some coordination. But because it hit so late, it really did not have the impact. But, again, responsible media, government warnings, and the reflection period all prevented something that, if it would have happened 72 hours before, may have had a different impact on that election.

Senator Rounds: Senator Gillibrand?

Senator Gillibrand: Thank you.

Just following up on a couple things. You said the Belfer Center already has done a deep dive on how we were hacked and ways to prevent it. Is that true?

Dr. Sulmeyer: Senator, the two reports are about the practices that campaigns and State and local officials can take based on field research about what they found as vulnerable and techniques that were effective in the past, so ways to shore up those defenses. It is not going to be that kind of a deep dive like you are --

Senator Gillibrand: Have you distributed that to the 50 States?

Dr. Sulmeyer: I believe so, yes.

Senator Gillibrand: Have you gotten comments or any response back?

Dr. Sulmeyer: It went live today.

Senator Gillibrand: So I would like to request that you brief this committee on what the responses are to each of those efforts to outreach the different States and a copy of the report for all committee members so that we have our own first draft of what our 9/11 deep dive might ultimately look like because this has to be done. And it is striking to me that there is no sense of urgency by this administration. It is absolutely crazy as far as I am concerned. And so I want to work towards elevating this issue, and your work will help us do that.

Dr. Harknett, you mentioned in your comments that bots do not have free speech rights. I could not agree with you more. So what kind of legislation do you think we could write or could be written to say we expect these platforms, whether it is Facebook or Twitter or Instagram or any other online community, to not sell its technology to fake entities who are posing as real people? And the reason I say that is it is simple fraud, as far as I am concerned, because you are doing it for the purpose of changing someone's mind, distracting them, giving them false information. And I believe it should be illegal under the same analysis that we have for fraud statutes. How would you go about trying to take away those free speech rights that are given to non-entities today?

Dr. Harknett: Thank you, Senator.

So I am not a lawyer, but I would build on what you just said. I think the notion of our default to fraud -- so if in fact what you are trying to sell is trend, if that is the actual operative thing that you are trying to -- then that actually should be capturing human behavior. And so we really have to think through -- I mean, this is very tricky. But legislatively we have to separate out human behavior from automated behavior, and automated behavior can be classified as falsification of trending, if you wanted to capsulize it in that fashion. So I think the notion of understanding technical manipulation of the space is not smart marketing. It is manipulation and therefore should be out of bounds.

Can I make one quick comment on your deep dive?

Senator Gillibrand: Yes.

Dr. Harknett: I would look as another example, Eisenhower's solarium exercises back in the 1950s. President Eisenhower said, okay, what is going to be our macro level grand strategy? Set up three competing teams to come up with what those strategies should look like, and that is where containment and deterrence came from. It is an interesting alternative approach, but we get at the same sort of things that you are looking at.

Senator Gillibrand: Like a national competition?

Dr. Harknett: Well, he brought together three very specific groups of experts. They were given access to classified information, but they worked as independent teams. And then they were brought together to knock heads over what the best route to a grand strategy looks like.

We do not have a cyber grand strategy, and we do not have a grand strategy for cyberspace. I can tell you the Chinese do. They have announced it. They are going to be the number one AI country by 2030. We need to start to think in those kinds of grand strategic terms.

Senator Gillibrand: Other thoughts?

Mr. Butler: Yes. Senator, I would build on the Honest Ads Act. You have got elements in this particular legislation which gets to what we want online platforms to do. They can identify botnet infrastructure and are beginning to identify infrastructure that has origin in elements that are nefarious. And so I think I would add to that as one way of kind of tackling this issue.

The second point. I do not want to disagree too strongly with my colleagues here, but I have worked in the private sector and I have worked on the public sector side. And I know that there are models that can work to align incentives. The enduring security framework is a good example of that. We have had it work before. When you show private sector and national security government elements

working together a threat of this magnitude and you provide some type of limited liability protection, you can get there. It took us a long time with Facebook, Twitter, and Microsoft to get to pulling terrorists' data offline, but they are doing it now. My sense is the sooner we get into this process with creating an alignment of not only incentives but understanding of the problem -- and again, it is not with everyone. It is with folks who can do things on scale and really help us as a nation.

Senator Gillibrand: Thank you.

Thank you, Mr. Chairman.

Senator Rounds: Thank you, Senator Gillibrand.

First of all, let me just take this time to say thank you very much to all of our witnesses for your time. You spent an hour and a half with us today. It has been greatly appreciated. I would suspect that we will be speaking again in the future as we continue to learn more about the challenges and the threats that face our country. It is not going to get better. It is going to get worse. We all recognize that. Our challenge is to make sure that we have the right long-term strategies and that they are being properly implemented. As such, I think we have got a lot of work to do.

With that, once again, thank you. Thank you for the participation of our members here today.

At this time, this subcommittee meeting is adjourned.

[Whereupon, at 3:53 p.m., the hearing was adjourned.]